UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,125	07/07/2003	Kyung-Hun Jang	249/387	7220

27849 7590 11/05/2007

LEE & MORSE, P.C.
3141 FAIRVIEW PARK DRIVE
SUITE 500
FALLS CHURCH, VA 22042

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
11/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/613,125	JANG ET AL.	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 28 August 2007, has been received, entered into the record, and respectfully and fully considered.

2. By this amendment, claims 12 and 21-23 are amended. Claims 24-25 are newly added claims. Therefore, claims 1-5, 7-18 and 20-25 are pending.

3. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

Election/Restrictions

4. Since the Applicant amended claims 21 and 23, they are parallel claims of 1 and 12. Therefore, the examiner withdraws restriction requirement. New claims 24 and 25 are entered.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 5 and 16, 21-22 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claims 5 and 16**, "a key distribution center function" is being recited. However, it is not clear whether this is the same as or different from "a key distribution center function" recited in claims 1 and 12.

As per claim 21, "between the remaining wireless terminals" has been recited. However, "the remaining wireless terminals" lacks of antecedent basis.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-5, 8-10 and 11-18, 21 and 23-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Asokan et al. ("Key agreement in ad hoc networks", Computer Communications, Volume 23, Number 17, 1 November 2000)

As per **claims 1 and 12**, Asokan et al. discloses a cryptographic method/system using dual keys in a wireless local area network (LAN) system, comprising:

(a) generating a first group key in N wireless terminals forming an ad-hoc group (an ad-hoc meeting –e.g. p1, "They would like to set up a wireless network session...for the during of the meeting"), where N is equal to or greater than two (P5, "There are two parties A and B which share a weak secret P" and P6 "We can slightly modify this....to a contributory multi-party protocol") ;

(b) generating a second group key in a main wireless terminal (a leader – e.g. P6) to perform a key distribution center function among the N wireless terminals, and transmitting the second group key to (N-1) sub wireless terminals (P6, "An additional round will...to pick a common session key and distribute it the members of the group....he shares with them"); and

(c) encoding data using the second group key, and transmitting the encoded data between the N wireless terminals (P4 "In a landmark paper [4], Bellovin and Merrit....encrypted key exchange (EKE) and P5 "But the basic form of the generic protocol remains the same." Inherently, Asokan et al. teaches after the protocol is complete, the multi parties must communicate using the session key (the second group key) to encoding data and transmitting the encoded data among the N wireless terminals since the protocol is using encrypted key exchange (EKE), a well known protocol invented by Bellovin and Merrit disclosed on the P4 of the Asokan et al. reference).

(d) modifying the second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal, and transmitting the modified second group key to the (N-1) sub wireless terminals (P5, "session key"- a session key is a key that is just used for one communication session and then discarded, Page 20, "multi-party key agreement will need to address the issues of synchronization and resilience in face of benign faults... and page 11, "at the end of the round, all four players will have the same key...", "The time needed will be the same as that of one two-party key exchange" – page 12, "Synchronous rounds could be

implemented if all nodes have loosely synchronized clocks" – page 12, "...key exchange can be done efficiently, in terms of the number of communication rounds.." – page 10, "The protocol proceeds through d rounds, 1,..., d." – page 11 and "...between themselves in k-1 rounds...In the end of those k-1 rounds each group will have a shared key. For all 2k members to agree on a single shared key in round k...**The time needed will be the same as that of one tow-party key exchange**. Notice in round 1...In round k,...doing key exchange in parallel" – page 12).

As per **claims 2 and 13**, Asokan et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the first group key is generated using a group password of the ad-hoc group (P3, "choosing a fresh password and sharing it among those present in the room, P4 "In a landmark paper [4]....encrypted key exchange (EKE)...derive a strong and P5 "shared key starting from only a weak shared key")

As per **claims 3 and 14**, Asokan et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal encodes the second group key using the first group key, and transmits the encoded second group key to the (N-1) wireless terminals (P5, "In step 1 A sends Ea encrypted with the weak secret P....At this point, each player will compute the session key as

K=f(Sa, Sb) and P6, "One obvious way....and distribute it to the members of the group using the pairwise session keys he shares with them") .

As per **claims 4 and 15**, Asokan et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal is a creator of the ad-hoc group (P 18, "for example,...the leader Mn has a greater say in the final session key...before finding one that leads to a particular type of K" and "In some ad-hoc networks there may already be a natural leader or ordering").

As per **claims 5 and 16**, Asokan et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further inherently discloses wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal (P16, "Therefore, when there is no a.priori leader or ordering...The general approach...This computation can be car- and P17, "ried out...to their distance from the reference value" and P20, "If groups are dynamic, the session key needs to updated when the composition of the group changes").

As per **claims 8 and 17-18**, Asokan et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses:

if the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal (Page 5, "B extracts Ea, generates R randomly, encrypts it with Ea, and returns it to A in step 2");

decoding the second group key request message, using the first group key, in the main wireless terminal (P5, "The goal of the protocol is for A and B to mutually authenticate each other based on P, and to agree on a strong session key K...each player will compute the session key as K=f(Sa, Sb)") ; and

creating a second group key according to the decoded second group key request message, in the main wireless terminal (P6, "an additional round...he shares with them").

As per **claim 9**, Asokan et al. discloses the claimed method of steps as applied above in claim 1. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 10**, Asokan et al. discloses the claimed method of steps as applied above in claim 3. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 11**, Asokan et al. discloses the claimed method of steps as applied above in claim 8. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 21 and 23**, they are rejected using the same rationale of rejecting claims 1 and 12 above.

As per **claims 24-25**, they are rejected using the same rationale of rejecting claims 1, 8, 12 and 17 above.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 7, 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asokan et al. as applied to claims 1-6, 8-10 and 11-19 and 21 above, further in view of Schneier ("Applied Cryptography" second edition, 1996)

As per **claims 7, 20 and 22**, the difference between the claimed invention and that disclosed in Asokan et al. is the latter does not disclose the claimed feature of the modified second group key is encoded using a non-modified second group key, and transmitting the encoded second group key to the (N-1) sub wireless terminals. However, such missing feature in Asokan et al. is clearly taught section 8.6 Updating keys on page 180, of the aforementioned Schneier reference, the same field endeavor of key management in the network enviroment. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Schneier reference into the Asokan et al. method motivated by to provide "an easier solution is to generate a new key from the old key" (Schneier, Section 8.6 on page 180)

Response to Arguments

13. Applicant's arguments with respect to claims 1-25 have been considered but are moot in view of the new ground(s) of rejection. Please note the new claim limitation "modification time period...predetermined in the main wireless terminal" in claims 1 and 12 is not recited in the canceled claims 6 and 19.

14. On page 14 of the remark, the Applicant states that the claims are now limited to tangible computer media as the spec no longer includes carrier wave. The examiner takes this a disavowal of that nonstatutory embodiment and withdraws the 101 rejections on claims 9-11.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

25 October 2007
AYS

KIM VU
SUPERVISORY PATENT EXAM.
TECHNOLOGY CENTER 2